ISMS.online

Stakeholder expectations – considerations for your information security management system (ISMS) business case.

Another major factor affecting the investment in the ISMS is to what extent it meets the needs and expectations of stakeholders, given their power to tell you what to do, and their interest in evidence of it being done.

The table below highlights examples of stakeholders. The common thread is about growing trust through exhibiting confidence and control, where that increases the more visible, insightful and well evidenced the ISMS becomes.

If you are unsure about a stakeholder's expectations from the ISMS perhaps ask them. Ensure that your ISMS is fit for the purpose now, as well as able to adapt and grow as this information security and privacy-oriented world changes (because it is changing fast!)

How long you spend on the evaluation is up to you. It should be based on the risks and rewards facing the organisation and the need to justify the case for investment to your powerful stakeholders.

Stakeholder	*Interest in the ISMS*	*Ability to evidence now?* *Yes / No / NA*
Leadership & Board	1. Protection of assets and ability to drive growth in organisation value with confidence in the ISMS 2. Ensuring that information security practice enables business success not prevents it 3. Able to visibly demonstrate the ISMS and build trust with powerful stakeholders 4. Certainty the ISMS is under control and working well at all times 5. The ISMS helps mitigate personal accountability risk as new legislation comes into force 6. The cost of ISMS investments and management of the solution is relative to opportunities and threats 7. Confidence that the ISMS is able to continue working well if people running it change or move on	
Shareholders	8. Confidence that the ISMS is working as expected 9. Protection and growth of shareholder value	
Regulators & Legislators	10. Confidence the ISMS enables privacy and protection of data subject information (e.g. GDPR) 11. Ability to see the actions taken and work done prior to and afterwards - in the event of a breach or reason to investigate *(which will influence their recommendations and outcomes)*	

Customers	12. Ensuring the organisation delivers on its promises and protects information being shared or processed 13. Evidence that the ISMS is working in the organisation 14. Assurance of the whole supply chain performing especially important suppliers accessing their assets	
External Auditors	15. Ensuring the organisation is running its ISMS according to any agreed standards (e.g. to meet customers' expectations) such as ISO 27001 16. Confidence in the operation going beyond 'tick box' and living the spirit of information security daily	
Employees	17. Protection of their own personal data 18. Reputation of the organisation to continue trading and employ them 19. Ease of demonstrating their personal ISMS awareness & compliance to aid organisation goals	
Suppliers & Partners	20. Confidence that the relationship is not leaving them exposed to risk given supply chain liability is increasing 21. Ability to learn from smart responsible customers & partners about how to protect their part of the supply chain	
ISMS management and administration resources	22. Ease of operation and ability to demonstrate to other stakeholders they are in control of the ISMS 23. Able to focus on 'what' they are doing for improving security and privacy rather than 'how' to build and develop an ISMS itself	
Trade associations / powerful lobby groups	24. Starting to set standards and expectations for organisations in their scope and see evidence of security and privacy best practices from members	

This is one of the templates provided in good faith to help you consider and evaluate the return on investment (RoI) from an Information Security Management System (ISMS).

If you would like more help with building your business case for an ISMS or are ready want to get your ISMS.online then please contact us at www.ISMS.online and organise your consultation.